Sanitized Copy Approved for Release 2010/11/17 : CIA-RDP87T00623R000200070025-2

DIRECTOR OF CENTRAL INTELLIGENCE
SECURITY COMMITTEE
COMPUTER SECURITY SUBCOMMITTEE

24 June 1983
DCISEC-CSS-M155

1. The One Hundred and Fifty-Fifth meeting of the Computer Security Subcommittee was held on 21 June 1983 at the [redacted] McLean, VA., and was attended by the following persons:

STAT [redacted] Executive Secretary
STAT [redacted] CIA
NSA
Mr. Lynn Culkowski, Air Force
Mr. David Schenken, U.S. Secret Service
STAT [redacted] Chairman, SECOM
STAT [redacted] CIA (observer)

2. In the absence of the Chairman, the meeting was chaired by the Executive Secretary. The first item discussed was the minutes of the previous meeting. Since there were no comments on the minutes, they were accepted as written.

3. The minutes of the previous meeting (DCISEC-CSS-M154) indicate
STAT briefings to be presented to [redacted] by the Subcommittee, on threat and the status of the rewrite of DCID 1/16. The Executive Secretary
STAT reported that briefings were presented to [redacted] on 3 June, with Capt.
STAT John Lilly of the 337th MI Detachment and [redacted] giving the threat
STAT briefing, and [redacted] discussing the status of the DCID rewrite.

4. There was a short discussion concerning the dichotomy between high level guidance and actual budgetary and resource decisions as they affect computer security programs. The problem appears to be that, although there is guidance which is supportive of computer security programs within DoD and the Intell. Community, in practice computer security billets are being lost. This is clearly putting a strain on ISSC programs, and on the ability to adequately implement and manage them. It was agreed that what is required is high level budgetary and resource guidance for computer security programs which would then allow the various agencies and departments to commit the resources necessary to carry them out.

5. The remainder of the meeting was largely dedicated to a review of the latest proposal of the DCID (briefed by the Executive Secretary at the last meeting, and distributed with the previous minutes). specifically, the discussion on the DCID covered the following points:

(a) There were no objections to either the overall structure (i.e., five modes of operation defined within three classes, or environments), or to the definitions of the classes (i.e., User, Data Sharing, and Process Sharing).

Sanitized Copy Approved for Release 2010/11/17 : CIA-RDP87T00623R000200070025-2

Sanitized Copy Approved for Release 2010/11/17 : CIA-RDP87T00623R000200070025-2

(b) It was noted that the new draft now defines the ISSO responsibilities in more detail and with more clarity, clearly demonstrating the full scope of the ISSO's responsibilities and duties. However, the issue was raised about the ISSO's ability to read, understand, and apply the technical details of the DCID. As a consequence, it was suggested that a description of qualifications for the ISSO be developed and included in the regulatory section of the DCID.

STAT (c) It was suggested by [redacted] that each of the members "test" the draft DCID within his own organization, through presentations or by choosing an operational facility to review or apply the document. This would be pursued as strictly a working level review to determine useablitly and acceptability; definitely not a policy level review. Specifically, the purpose of this review is to elicit questions, general reactions, comments, and to identify systems which can (and cannot) fit the "classes" described, as well as to determine the ease or difficulty of applying the document. It was agreed that each member will be responsible for carrying out the review within his own department/agency, and be prepared to submit the results by the September meeting. (It was noted that it is probably wise to touch base with the policy elements to let them know what is going on).

(d) There was some concern raised over the wording of the "Authority" paragraph of the basic policy document, in particular, that dealing with "Multiple NFIB Member's System/Network". It was pointed out that this section needs to distinguish between "sharer" and "customer".

(e) The question was raised concerning satisfying the requirement for "per-user" accountability in the communications environment; if there are strong physical/personnel/procedural security measures in place at the terminal sites, can those take the place of the accountability requirements which appear to be demanded for the hardware/software?

(f) The other significant point raised was the question of whether or not the document was intended to also apply to circuit switches, PBX'es, etc. If so, then some careful review of the wording may be in order.

(6) The next meeting was scheduled for 0930 on 19 July at the

STAT [redacted] McLean VA.

STAT [redacted]

Executive Secretary

Sanitized Copy Approved for Release 2010/11/17 : CIA-RDP87T00623R000200070025-2